UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,586	06/19/2006	Benjamin Morin	33901-200PUS	1443

27799 7590 08/27/2009

COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
08/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/583,586	MORIN ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-10,12 and 13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-10,12 and 13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 06/12/2009.

2. Claims 1 and 12 have amended.

3. Claims 1, 3-10 and 12-13 are pending for consideration.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/12/2009 has been entered.

Response to Arguments

5. Applicant has canceled claim 11, therefore the 35 U.S.C. 101 rejection has been withdrawn.

6. Applicant's arguments with respect to claims 1, 3-10 and 12-13 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3-10 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Julisch ("Clustering Intrusion Detection Alarms to Support Root Cause Analysis") (hereinafter Julisch) in view of Kidder et al. (US 6445774) (hereinafter Kidder).

9. Regarding claim 1, Julisch discloses a method of managing alerts (Julisch: pages 467-468) issued by intrusion detection sensors of an information security system including an alert management system, each alert being defined by an alert identifier and an alert content, which method includes the following steps: associating with each of the alerts issued by the intrusion detection sensors a description including a conjunction of valued attributes belonging to attribute domains (Julisch: page 449, paragraph 2, "where {A1,…, An} is the set of alarm attributes … alarm attributes capture intrinsic alarm properties, such as the source IP address or an alarm, its destination IP address, its alarm type (which encodes the observed attack), and it time-stamp"); organizing the valued attributes belonging to each attribute domain into a taxonomic structure defining generalization relationships between said valued attributes, a plurality of attribute domains forming a plurality of taxonomic structures (Julisch: page 449, paragraphs 2-4, "dom(Ai) is the domain (i.e., the range of possible value) of attribute Ai" and "generalization hierarchies"); completing the description of each of said alerts with sets of values induced by the taxonomic structures based on the valued attributes of

said alerts to form complete alerts (Julisch: page 449, paragraphs 2-4, "generalized alarm"); storing said complete alerts in a logic file system to enable said complete alerts to be consulted (Julisch: page 450, section 4 [ALARM-CLUSTERING PROBLEMS] and pages 456-457, section 5.1 and 463-465, "alarm log"); wherein each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic (Julisch: pages 449 and 460-463).

Julisch does not explicitly disclose consulting the complete alerts by at least one of successively interrogating and browsing said complete alerts so that the alert management system responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request to enable said request to be refined, said request being a logic formula of at least one of said valued attributes.

. However, Kidder discloses consulting the complete alerts by at least one of successively interrogating and browsing said complete alerts so that the alert management system responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request to enable said request to be refined, said request being a logic formula of at least one of said valued attributes (Kidder: column 8 line 63 through column 9 line10 and column 12 lines 37-64). Therefore, it would have been obvious to a person skilled art at the time the invention was made to have included in Julisch the feature of Kidder as discussed above because current network monitoring environments have not sufficiently reduced the response period to achieve this level of

responsiveness. As discussed above, current network monitoring environments are very limited in the features they provide for network monitors, and such network monitoring environments cannot be easily tailored to accommodate the workflow of network monitors (Kidder: column 4 lines 1-9).

10. Regarding claim 3, Julisch as modified further discloses wherein the pertinent valued attributes assigned a highest priority are those that are most general, given the taxonomic structures (Julisch: page 464).

11. Regarding claim 4, Julisch as modified further discloses wherein the alert management system further responds to the request by supplying alert identifiers satisfying the request and whose description cannot be refined with respect to said request (Julisch: pages 464-465 and 467-468, section 7).

12. Regarding claim 5, Julisch as modified further discloses wherein the alert identifier is a pair consisting of an identifier of the intrusion detection sensor that produces the alert and an alert serial number assigned by said intrusion detection sensor (Julisch: pages 449 and 452).

13. Regarding claim 6, Julisch as modified further discloses wherein the content of each alert includes a text message supplied by a corresponding intrusion detection sensor (Julisch: pages 451-452).

14. Regarding claim 7, Julisch as modified further discloses wherein each valued attribute includes an attribute identifier and an attribute value (Julisch: pages 449 and 451-452).

15. Regarding claim 8, Julisch as modified further discloses wherein each attribute identifier is associated with one of the following attribute domains: attack domain, attacker identity domain, victim identity domain and attack date domain (Julisch: pages 449 and 451-452).

16. Regarding claim 9, Julisch as modified further discloses wherein the description of a given alert is completed by recovering recursively from generalization relationships of the taxonomic structures a set including more general valued attributes not already included in the description of another alert completed previously (Julisch: pages 449 and 456, last paragraph).

17. Regarding claim 10, Julisch as modified further discloses wherein the valued attributes in the taxonomic structure are organized in accordance with an acyclic directed graph (Julisch: pages 449 and 462).

18. Regarding claim 12, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

19. Regarding claim 13, Julisch as modified further discloses Information security system comprising intrusion detection sensors and the alert management system according to claim 12 (Julisch: page 467-468).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431